FIREEYE

ONE
IT ONLY TAKES ONE EMAIL FOR A CODE TRIAGE

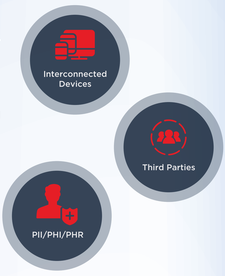
281 billion emails are sent each day.[1]

Every day, attackers send a whopping 150 million phishing emails. If printed and laid end-to-end, these malicious messages would stretch over 26,000 miles—far enough to circle the earth.

Why Healthcare is Under Attack

FireEye is currently tracking 17 advanced threat groups targeting healthcare, including providers and facilities, insurance, medical equipment, pharmaceutical, biotechnology and social services. Spear phishing and strategic web compromises are the most common attack vectors we see in healthcare, which is among the most frequently targeted industries that suffered significant attacks last year.[2]

- Healthcare records fetch the biggest payoff
- Interconnected devices often run on outdated systems and/or in the cloud
- Health information exchanges with third parties provide countless access points



32% of all emails received are clean.[3]

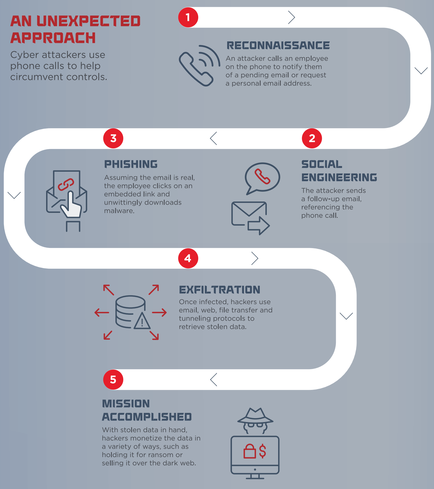
91% Almost all cyber crimes start with email.[4]

84% A majority of organizations have been spear phished.[5]

The Path of an Attack

AN UNEXPECTED APPROACH

Cyber attackers use phone calls to help circumvent controls.



95% of phishing-based breaches are followed by software installation.[5]

The Costs of an Email Breach

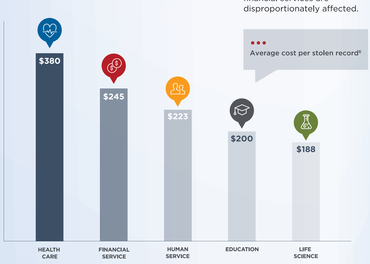
FINANCIAL COST
$3.62M
Average cost of an email breach

REMEDIATION TIME
66 days
Average time required to contain the breach

RECURRENCE RATE
27.7%
Likelihood a second material data breach will occur within 24 months[5]

INDUSTRY MOST IMPACTED BY CYBER THREATS

On average globally, a breach costs $141 for each stolen record, but some industries such as health care and financial services are disproportionately affected.



Incident response teams and the extensive use of encryption **reduce the cost of a data breach by as much as $19 per compromised record.[6]**

FireEye Email Security means better protection

Safeguard your organization's business assets against phishing and ransomware.

Get real-time, automated protection from spear-phishing and other socially engineered attacks.

Stay secure, whether your email environment is on-premises, cloud-based or a hybrid.

Rest assured with always up-to-date protection; no upgrades needed.

Respond to threats more effectively with comprehensive, contextual threat intelligence.

Protect your organization from hard-to-detect multi-vector, multi-flow attacks.

Protect your people, data and assets with FireEye Email Security. Learn how at **www.FireEye.com/email.html**

- Reduces business risk of unauthorized access
- Saves operational costs
- Deploys in minutes with no physical infrastructure

1 Radicati Group (February 2017). Email Statistics Report, 2017-2021.
2 FireEye (2019). M-Trends 2019.
3 FireEye (August 2018). Get One Step Ahead of Email Threats, Email Threat Report for January–June 2018
4 PhishMe (2016). Enterprise Phishing Susceptibility and Resiliency Report
5 Vanson Bourne (2016). The Impact of Spear Phishing.
6 Ponemon Institute LLC (June 2017). "2017 Cost of Data Breach Study: Global Analysis."

E-EXT-10-US-EN-000102-02

FIREEYE